

UNITED STATES DISTRICT COURT

FILED

WESTERN

for the
DISTRICT OF

OKLAHOMA

In the Matter of the Search of

1613 Westwood Ln.
Edmond, Oklahoma 73013

Case No: M- 20-409-STE



4:57 pm, Aug 26, 2020
CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA
By: Andrea Caster, Deputy Clerk

APPLICATION FOR SEARCH WARRANT

I, Marisol Flores, a Special Agent with the Federal Bureau of Investigation (FBI), request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A, which is incorporated by reference herein.

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B, which is incorporated by reference herein.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252A(a)(5)(B)

Offense Description

Possession of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Marisol Flores, Federal Bureau of Investigation, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of [No. of Days] days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Marisol Flores
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: Aug 26, 2020

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge
Printed name and title

**THE UNITED STATES DISTRICT COURT FOR THE WESTERN
DISTRICT OF OKLAHOMA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Marisol Flores, a Special Agent (SA) with the Federal Bureau of Investigation (FBI),

being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since May 2015, and I am currently assigned to the Oklahoma City Division. Since joining the FBI, I have been involved in investigations of child exploitation matters and computer crimes against children. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as an SA with the FBI.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. I am investigating the online activities of Bradley Kerns, who resides at 1613 Westwood Ln, Edmond, OK 73013. As shown below, there is probable cause to believe that Kerns has received, possessed, and distributed child sexual abuse material, in violation of 18 U.S.C. § 2252. I submit this Application and Affidavit in support of a search warrant authorizing a search of Bradley Kerns' residence, located at 1613 Westwood Ln, Edmond, OK 73013, hereinafter referred to as the "SUBJECT PREMISES," as further described in Attachment A. Located within the premises to be searched, I seek to seize evidence, fruits,

and instrumentalities of the foregoing criminal violations. I request authority to search the entire premises, including the residential dwelling, the curtilage of the residence, including, but not limited to storage buildings, vehicles located on the premises, the person of Bradley Kerns, provided that he is located within the premises at the time of the search, and any computer (as broadly defined in 18 U.S.C. 1030(e) or any other digital file storage device) located therein, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

4. The statements in this Affidavit are based in part on information provided by the Federal Bureau of Investigation (FBI), Milwaukee Division (MW), and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252 are presently located at the SUBJECT PREMISES.

5. I am also aware that computers and computer-related media are portable and that evidence can be stored on media as small as a fingernail-sized memory card. I have learned from other law enforcement officers who have executed search warrants in investigations of this nature, and my own training and experience, that computers and digital devices containing child sexual abuse material can be located in vehicles and on the persons of occupants located on the premises. In addition, I am aware that people frequently transport their computers and cellular telephones on their person and in their vehicles. Due to the portable nature of electronic storage devices and the ease with which

they can be transported and hidden, I am requesting authority to search any vehicles on the SUBJECT PREMISES which Kerns is known to drive, as well as the person of Bradley Kerns, provided that he is located on the premises. Thus, the term “SUBJECT PREMISES” includes vehicles registered in Kerns’ name as well as Bradley Kerns’ person, provided that they are located on the premises when the search warrant is executed.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. “Child Sexual Abuse Material” includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

See 18 U.S.C. § 2256(8).

c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” *See* 18 U.S.C. § 1030(e)(1).

d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

i. “Peer-to-peer file-sharing” (P2P) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, and conducting searches for files that are currently being shared on another user’s computer.

j. “Sexually explicit conduct” applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality;

(c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

k. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

l. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD SEXUAL ABUSE MATERIAL

7. Based on my knowledge, training, and experience in child exploitation and child sexual abuse material investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology,

and the Internet have revolutionized the manner in which child sexual abuse material is produced and distributed.

8. Computers basically serve four functions in connection with child sexual abuse material: production, communication, distribution, and storage.

9. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child sexual abuse material. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet affords collectors of child sexual abuse material several different venues for obtaining, viewing, and trading child sexual abuse material in a relatively secure and anonymous fashion.

12. Collectors and distributors of child sexual abuse material also use online resources to retrieve and store child sexual abuse material, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an

online storage account from any computer with access to the Internet. Evidence of such online storage of child sexual abuse material is often found on the user's computer. Even in cases where online storage is used, however, evidence of child sexual abuse material can be found on the user's computer in most cases.

13. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data. Likewise, devices such as cellular telephones, tablets, and e-readers are also capable of electronic storage as computers.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

14. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related

documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

15. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child sexual abuse material where the evidence consists partly of graphics files, the

monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

16. Furthermore, I know that smart cell phones (a type of “computer,” as broadly defined in 18 U.S.C. § 1030(e)) can typically “sync” with a traditional desktop or laptop computer. The purpose of syncing a smart phone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smart phone is lost or damaged. Also, smart phone users may move files off the smart phone and onto a computer to free up storage space on the smart phone. Similarly, computer (e.g., desktop computers, smart phones, etc.) users may move files off of one computer onto another computer or digital file storage devices such as a thumb drive, a DVD, an external hard drive to free up space on the computer. For this reason, I am seeking authorization to seize all computers and digital file storage devices at the SUBJECT PREMISES—not any particular computer. Finally, I know that many modern smart cell phones, including Apple iPhones and Samsung-brand phones, can be encrypted by the user using his finger and/or thumbprints to lock and unlock the device. Without the user's prints, the devices are difficult, if not impossible, for law enforcement personnel to unlock. Accordingly, I am requesting that, to the extent law enforcement seizes any smart cell phones or other computers described in Attachment B during a search of the SUBJECT PREMISES (described in Attachment A), and if such device(s) features such encryption, then law

enforcement may, while executing the search warrant at the SUBJECT PREMISES, depress the occupant(s) of the SUBJECT PREMISES finger and/or thumbprints onto any such encryption feature to attempt to unlock the device.

BACKGROUND OF THE INVESTIGATION

17. On March 11, 2020, an FBI MW undercover employee (hereinafter referred to as “UCE”) logged onto a cellphone application, used for messaging, named Kik Messenger (hereinafter referred to as “Kik”). Within the Kik application, the UCE entered the private group, “Group A,”¹ after being previously added from a public group in Kik. The private group, “Group A,” had been established as a child sexual abuse material sharing group on Kik. Multiple images and videos of child sexual abuse material have been shared with members of the group. While in the private group, “Group A,” the UCE observed an individual utilizing the username, “allgravy1,” as a member of the group. At approximately 9:58 pm, on March 11, 2020, “allgravy1” sent a video, “IMG_3668”, to the group, “Group A,” depicting two nude prepubescent females (pre-female A, and pre-female B), approximately 5 to 6 years old in a bathtub with an adult male. The bathroom and bathtub are both white in color. Pre-female A is sitting in the bathtub facing the adult male and engages in oral sex, while pre-female B sits behind pre-female A. Later, pre-female B moves in front of pre-female A and lays on the adult male’s chest. The adult male grips either side of pre-female B’s butt cheeks and places his penis in-between. Near the end of the video, pre-female A, with pre-female B still lying on the adult male, comes

¹ Due to the ongoing nature of this investigation, “Group A” is being used to identify a specific group within Kik which the UCE was part of. “Group A” is not the true name of the group.

forward and again engages in oral sex with the adult male. In addition, I observed what appeared to be camera flashes during the video and the shadow of an additional person observed on the wall. On March 25, 2020, at approximately 11:02 pm, “allgravy1” sent another video, “IMG_3954”, to the Kik group, “Group A” depicting an adult male, without any visible clothes, inserting his erect penis into a prepubescent female’s anus while she was laying down. The prepubescent female is wearing white and purple underwear and is lying on a yellow covered sheet or blanket.

18. In response to a subpoena by law enforcement, Kik identified the username, “allgravy1” to have subscriber information as follows:

First Name: B

Last Name: K

E-mail: bradjkerns@gmail.com (confirmed)

Also, according to Kik records, the majority of connections between March 15, 2020², and April 13, 2020, occurred from IP address 98.162.206.55 and several occurred from IP address 70.182.81.253. IP address 98.162.206.55 resolved back to Cox Communications and IP address 70.182.81.253 resolved back to a Cox Communications Business account. In addition, Kik records also revealed “allgravy1” registered the Kik account from an iPhone with the email, bradjkerns@gmail.com.

Pursuant to a subpoena, Cox Communication provided information in regards to IP address 98.162.206.55 between the dates of August 2, 2018, to May 15, 2020, as follows:

² Kik provides IP information for up to thirty days prior from subpoena receipt date. The Kik subpoena was received on April 13, 2020, therefore their records only went as far back, in regards to IP addresses, to March 13, 2020.

Name: Jeanette Harder

Address: 1613 Westwood Ln, Edmond, OK

Home Phone: 405-650-2703

Pursuant to a subpoena, Cox Communications provided information in regards to IP address 70.182.81.253 between the dates of August 2, 2018, to May 15, 2020, as follows:

Name: Prestige Worldwide Corals

Address: 8019 NW 23rd St., Bethany, Oklahoma

Home Phone: 405-206-9230

Pursuant to another subpoena, Google produced records associating "bradjkerns@gmail.com" with the name "Brad Kerns," Recovery SMS, +4054142685, and Sign-in Phone Number, +4054142685. Additionally, according to Google records, there was one login from IP address 98.162.206.55 on February 9, 2020.

In response to an additional subpoena sent to AT&T, telephone number 405-414-2685 has subscriber information as Bradley Kerns with an address of 1613 Westwood Ln, Edmond, OK, 73013.

19. Open source research revealed Bradley Kerns is the son of Jeannette Harder, and both Kerns and Harder are residents of 1613 Westwood Ln, Edmond, OK, 73013.

20. On August 19, 2020, I verified through the U.S. Postal Service that Bradley Kerns currently receives mail at the SUBJECT PREMISES, with a postal address of "1613 Westwood Ln Edmond, OK 73013".

21. On August 13, 2020, investigators conducted physical surveillance at the SUBJECT PREMISES and observed a gray Dodge Ram truck, bearing Oklahoma license plate JBN-833, registered to Fowler Dodge, PO Box 720728, Norman, Oklahoma, parked on the curb in front of the residence from approximately 4:50 am to 8:00 am³.

22. On August 14, 2020, investigators conducted physical surveillance at Prestige Worldwide Corals, 8019 NW 23rd St., Bethany, Oklahoma. During surveillance, investigators observed a male, matching the description of Bradley Kerns⁴, working inside the business. Agents also observed the gray Dodge Ram truck, bearing Oklahoma license plate JBN-833, parked outside the business.

23. On August 19, 2020, investigators conducted physical surveillance at the SUBJECT PREMISES and observed a male, matching the description of Bradley Kerns, exit the SUBJECT PREMISES from the front door and enter in the gray Dodge Ram truck, bearing Oklahoma license plate JBN-833 and depart the SUBJECT PREMISES.

BACKGROUND AND USE OF THE “KIK MESSENGER

24. Kik Messenger, also known as “Kik,” is a popular free instant messenger application (app) for mobile devices (i.e., smart cell phones, tablets, iPods, etc.) from the Canadian company, Kik Interactive, which was founded in 2009. Kik is available on several mobile device platforms including, iOS, Android, and Windows Phone operating systems. The Kik application can be located through Google’s, “Play Store,” and Apple’s, “App Store.” The Kik application utilizes the internet connection through the mobile

³ At this time, surveillance was terminated and investigators left the area. This is not when the vehicle departed the residence.

⁴ Investigators had access to Bradley Kern’s driver’s license photo and identifiers of Bradley Kerns.

devices' data plan or through Wi-Fi, to transmit and receive messages, photos, videos, sketches, mobile web pages, and other content transmitted by through the Kik application. Kik allows its users to register a user account without providing a telephone number and prevents users from being located on the service through any information other than their chosen unique Kik username. According to Kik Interactive, Kik Messenger has approximately 300 million registered users and is used by approximately 40 percent of United States teenagers.

25. Based on Kik's website, "Kik has become the best way to connect with friends, no matter where you meet them. And unlike other messengers, Kik uses usernames - not phone numbers - as the basis for Kik accounts, so our users are always in complete control of who they talk to on Kik."

26. After locating the Kik application and downloading the application to the mobile device, the application requests permission to access the following data on the mobile device during the installation process; In-app purchases, Identity, contacts, Location, Photos/Media/Files, camera, Microphone, Device ID & call information. Once given permission by the user, the Kik application installs itself on the mobile device. After installing the Kik app on the mobile device and initializing the Kik application for the first time, the potential user is required to establish a Kik account and is prompted to select the "SIGN UP" option. While establishing a Kik account, the potential user is prompted to provide information, including the user's "First Name," "Last Name," and "Birthday." The potential user is prompted to create a "Kik Username," (which is the only information that

is required to be unique,) and is prompted to provide an “Email address.” The information provided by the potential user is used to establish a Kik account; however, this user information is not verified, and the information can be completely fictitious (except for the uniqueness of the Kik username). A “verification email” is sent by Kik to the user’s provided email address and the user is prompted to verify the email address. Verification of the user’s email address is not required and does not prevent the user from utilizing the application if not verified. The potential Kik user is prompted to provide a user profile picture, which can either be taken using the mobile device’s camera feature or uploaded from the device photo gallery. However, the lack of a profile picture does not prevent the user from utilizing the application. The Kik username is created by the user and is the only information that is required to be unique.

27. At the completion of the account registration, the user is allowed to start communicating with other Kik users. Searching for specific Kik users can only be performed using the Kik user’s registered “username;” searches by phone number or email address cannot be performed. Entering the unique Kik username through the application’s search field yields potential matches in which the user simply selects the Kik user to start communicating with that specific user.

28. In today’s world where mobile phones are the technology of choice for millions of people to communicate, chat applications like Kik Messenger are often used to communicate with others, and on occasions are used during the commission of crimes, like the online harassment and bullying of juveniles, and the sexual exploitation of minors.

Mobile devices which utilize social media and communication applications, store, or “cache,” certain data from the social media or communication applications directly on the mobile device and this data can be recovered by a forensic expert. The Kik Messenger application is no different.

29. For both iOS and Android devices, most Kik artifacts relevant to criminal investigations are stored within specific databases located in specific locations on the mobile devices. These databases store details concerning the Kik users’ contacts, messages, and attachments sent and received through the Kik Messenger application. These databases contain such data as the usernames and display names for each contact but are not limited to this type of information. The Kik username is a unique identifier for each and every Kik user and this type of data is valuable in criminal investigations. The Kik contact database can also contain profile picture links and timestamps, as well as group and block lists. This data can be recovered from the mobile device by trained computer experts.

30. Messages, including any attached image files, are stored within a specific location on the mobile device, depending on the device used. As Kik stores all of its data in this specific location within the mobile device, in an unencrypted format, there is a good chance that the entire messaging history, if not a partial message history, can be recovered by trained computer experts and used during investigations.

31. Users sometimes delete their conversation histories by clearing the Kik Messenger logs. However, since the Kik messaging databases are not wiped or erased

immediately (depending on the operating system of the mobile device), these deleted records end up being stored in a specific location in a specific format on the mobile device. These deleted records may be kept for a period of time until the database reclaims the space to store new records. A forensic expert has the ability to recover such records which could prove useful in various investigations.

32. Sometimes, a user will attempt to destroy evidence by deleting the database file completely. While there is nothing that can be done to recover this information from an iOS device (the operating system does not allow for the recovery of anything that has been deleted), carving Android and chip-off dumps may return an amazingly high amount of deleted evidence.

CHILD SEXUAL ABUSE MATERIAL COLLECTOR CHARACTERISTICS

33. The following indicates characteristics of child sexual abuse material collectors that this Affiant has learned through training, working multiple investigations involving child sexual abuse material, and from other law enforcement officers with a background in child sexual abuse material investigations:

a. The majority of individuals who collect child sexual abuse material are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child sexual abuse material collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual

gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child sexual abuse material but which nonetheless fuel their deviant sexual fantasies involving children.

c. The majority of individuals who collect child sexual abuse material often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child sexual abuse material and child erotica as a means of gaining status, trust, acceptance, and support. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

d. The majority of individuals who collect child sexual abuse material maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

e. The majority of individuals who collect child sexual abuse material often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be

maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. The majority of individuals who collect child sexual abuse material rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes or other secure location.


CONCLUSION

34. Based on the aforementioned factual information, this Affiant respectfully submits that there is probable cause to believe that Bradley Kerns, residing in the SUBJECT PREMISES is involved in the possession, receipt, and distribution of child sexual abuse material, in violation of Title 18 U.S.C. § 2252. Additionally, there is probable cause to believe that evidence of those criminal offenses is located in the SUBJECT PREMISES, and this evidence, listed in Attachment B to this Affidavit, incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

35. This Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.



MARISOL FLORES
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Signed and sworn before me this  day
of August, 2020. 26th



SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE